Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of	)	WC Docket No. 16-106
Broadband and Other Telecommunications	)	
Services	)	
	)	

REPLY COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION

Steven K. Berry
President & CEO

Rebecca Murphy Thompson
EVP & General Counsel

Elizabeth Barket
Law & Regulatory Counsel

COMPETITIVE CARRIERS ASSOCIATION
805 15th Street NW, Suite 401
Washington, DC 20005
www.ccamobile.org

July 6, 2016

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

REPLY COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION

Competitive Carriers Association ("CCA") submits these reply comments in response to comments filed to the Federal Communication Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking ("NPRM") issued in the above-captioned proceeding.[1]

I. INTRODUCTION AND SUMMARY

The record in response to the Commission's proposed privacy rules on broadband Internet access service ("BIAS") providers depicts a resounding consensus that the Commission has failed to strike an appropriate balance of protecting consumers while promoting business. While the Commission has an undeniable interest in protecting consumers from privacy abuses, as do competitive carriers, the Commission should do so through a much broader, principles-based set of regulations, targeting abuses of sensitive data and giving consumers more control over that sensitive data. CCA approaches reply comments from a solutions-oriented perspective. Drawing from our membership as well as the FTC Consumer Protection Bureau Staff's helpful

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking*, Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016) ("NPRM").

comments,[2] CCA suggests a number of modifications to the FCC's proposed rules to improve the likelihood of consumer protection without overly taxing the ability of BIAS providers, especially non-nationwide providers and smaller providers, to operate effectively and produce innovative services and products.

CCA members are competitive carriers whose services span rural, regional, and nationwide areas. CCA represents nearly 100 competitive carriers, the vast majority of which are small businesses. CCA also represents nearly 200 affiliate members comprising vendors, equipment manufacturers, and other third-party service providers who are strong links in the overall chain of mobile broadband service provision. Regardless of service area or number of employees, CCA members compete in a consolidating industry wherein transparency and customer trust are distinct competitive advantages, and innovative services coupled with competitive pricing determines marketplace longevity.

The proposed privacy rules would undercut competitive carriers' ability to create and promote innovative services and, most importantly, hinder their ability to simply operate on a day-to-day basis. As the record amply supports, the proposals skew against small providers that would be unduly challenged to assume the various fees and burdens necessary to comply. Under the notice-driven proposals, consumers would be likely to tire of, and discard, notices from their BIAS regarding non-sensitive information, or endless requests for consent; this makes consumers less safe, and would chill innovation within the Internet economy.

In comments, CCA laid out a flexible privacy framework harmonized with the well-established and successful FTC framework, backed up by strong but fair enforcement for unfair

[2] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 15-106, *et al.* (filed May 27, 2016) ("FTC Comments").

or deceptive acts or practices ("UDAP") that materially harm consumers ("Industry Framework"). The Industry Framework sets forth a viable privacy solution that would safeguard consumers while blending seamlessly with existing privacy regimes throughout the Internet.[3] The record reflects a regime based on the Federal Trade Commission's ("FTC") unfairness and deception approach that is focused on the sensitivity of customer information and how the information is used, would best secure consumer protections while promoting innovative uses of data. Unfortunately, the proposed rules place an undue focus on controlling specific aspects of BIAS provider, and only BIAS provider, operations.

In response to the comments, below are targeted recommendations for revision that would more closely align the proposed rules with the FTC's hallmark flexible, context-based standards governing the rest of the Internet, including how to tailor rules regarding: (1) the overwhelming burden the proposed rules would impose on small providers; (2) customer proprietary information, and the scope of information covered by the rules; (3) data security; (4) data breach; (5) a customer choice framework; (6) notice and transparency; (7) third parties; (8) a small provider exemption; and (9) consistency and competition in the Internet marketplace. With these recommendations, the FCC will achieve its laudable goal of protecting consumer while promoting innovation and competition.

II. OPPRESSIVE COMPLIANCE BURDENS ON SMALL PROVIDERS JUSTIFY REVISING THE PROPOSED RULES

The Commission cannot conscionably adopt the proposed rules considering the crushing compliance burden they impose on small carriers. CCA dedicated the vast majority of its initial

[3] *See Ex Parte* Letter from Steven K. Berry, President & CEO, CCA, *et al.*, to the Honorable Tom Wheeler, Chairman, FCC, and attached Discussion Paper (March 1, 2016) ("Industry Framework").

comments in this proceeding to addressing potential harms to small providers, as did many other parties.[4] Special attention should be paid to the Small Business Administration Office of Advocacy's recent *ex parte* letter, agreeing that the "FCC's proposal would have significantly disproportionate economic impacts on small BIAS providers if finalized," and noting that the "record in this proceeding would support any effort by the FCC to mitigate the disproportionate compliance burden its proposal would have on small BIAS providers."[5] Small providers' constraints are not to be underestimated; complying with many of the proposed regulations could imperil the stability of a small provider's business.[6] This is especially concerning because small carriers generally do not share third party data.[7]

As summarized robustly by the American Cable Association ("ACA"), whose small cable operator members face many of the same operational and cost challenges as small mobile BIAS providers, small providers could not comply with the proposed rules without struggling with the cost of many factors, for example:

---

4 *See, generally,* Comments of Competitive Carriers Association, WC Docket No. 16-106 (filed May 27, 2016) ("CCA Comments"); *see also* Comments of NTCA – The Rural Broadband Association, WC Docket No. 16-106 (filed May 27, 2016) ("NTCA Comments"); *see also* Comments of WTA – Advocates for Rural Broadband, WC Docket No. 16-106 (filed May 27, 2016) ("WTA Comments"), *see also* Comments of American Cable Association, WC Docket No. 16-106 (filed May 27, 2016) ("ACA Comments"); *see also* Comments of Wireless Internet Service Providers Association, WC Docket No. 16-106 (filed May 27, 2016) ("WISPA Comments"); *see also* Comments of Rural Wireless Association, Inc., WC Docket No. 16-106 (filed May 27, 2016) ("RWA Comments").

5 *See Ex Parte* Letter from Darryl L. DePriest, Chief Counsel for Advocacy, SBA Office of Advocacy, and Jamie Belcore Saloom, Assistant Chief Counsel, SBA Office of Advocacy, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2, 4 (filed June 27, 2016) ("SBA Letter").

6 *Id.* at 4.

7 *See* CCA Comments at 33-34; *see also* RWA Comments at 9.

> attorney and consultant costs associated with regulatory analysis, contract negotiation, risk management assessments, and preparing required policies, forms, training, and audits; development and implementation costs associated with data security controls, website policies, and customer approval tracking systems; personnel costs associated with dedicated privacy and data security staff; costs associated with all aspects of providing required notices and follow-up; third-party costs associated with modifying contracts and ensuring compliance for call centers, billing software, and others that interface with customer proprietary information; and opportunity costs associated with diverting scarce resources from innovation and infrastructure deployment to regulatory compliance.[8]

Legal costs associated with privacy rules compliance would be an ongoing effort,[9] compounded by the larger list of growing compliance costs a BIAS provider must cover as Internet regulation grows more complex.[10] There is a high likelihood these surplus costs could not be absorbed by small carriers and instead they would have to pass on to consumers.[11] This does not serve

---

8 *See* ACA Comments at iii, 22; *see also* WISPA Comments at 26 ("Existing privacy policies may need to be revised to change 'opt-in' and 'opt-out' categories, with the assistance of legal counsel. Employees will need to be retrained, at the expense of lawyers, accountants or consultants. Someone will have to learn how to be a compliance officer, or have to hire a privacy professional to serve in that capacity. And someone will have to know when a data breach occurs, who to notify and when").

9 *See* WISPA Comments at 26 ("[L]arge companies with in-house lawyers and compliance officers can rely on those existing resources to re-write privacy policies, but small providers do not have in-house lawyers or regulatory departments and must hire outside counsel to advise on the new rules, draft new privacy policies, and conduct training").

10 *See* ACA Comments at 8 ("[T]hese privacy and data security costs do not exist in a vacuum—they are just one part of an increasingly complex web of legal and regulatory obligations with which providers must comply, including law enforcement, disabilities access, copyright, emergency alert service, universal service, and open Internet obligations, as well as a variety of state and local regulations").

11 *See* WISPA Comments at 27 ("These additional compliance costs cannot be absorbed by small businesses and will likely be passed on to consumers in the form of higher prices. Of critical importance, the Commission provides absolutely no economic analysis to document support for its prescriptive plan, but it is easy to imagine that those costs will be extremely burdensome"); *see also* Comments of CTIA, WC Docket No. 16-106 at 101 (filed May 26, 2016) ("CTIA

consumer welfare, especially considering many small businesses serve low-income or rural consumers and often times are the only provider.

The Commission should have explored the economic impact its proposed rules might have on small providers under Section 607 of the Regulatory Flexibility Act ("RFA"), which "requires agencies to develop a quantitative analysis of the effects of a rule and its alternatives using available data."[12] Further, the Commission should have included an analysis of significant alternatives to the proposed rule pursuant to Section 604 of the RFA.[13] The RFA analysis in the NPRM, however, was limited to descriptions of compliance requirements, and solicitations for comment on compliance costs.[14] CCA joins the SBA Office of Advocacy's call for the Commission to fulfill its obligations under the RFA and, in future filings, "include a discussion of all alternatives raised by small business representatives in the record, and explain its reasoning for adopting or declining to adopt each alternative."[15]

The rules, as proposed, should be amended to provide relief to small providers without compromising consumer protection. The most impactful revision is to the Commission's proposed definition of "customer proprietary information," or "customer PI," a category of information covering both the proposed definitions of CPNI and personally identifiable

---

Comments") (ISPs contending with overlapping self-regulatory and legal requirements governing privacy notices and policies may ultimately pass on added costs to consumers).

12 SBA Advocacy Letter at 2, *citing* 5 U.S.C. § 607.

13 *Id*. at 3, *citing* 5 U.S.C. § 604.

14 NPRM at 128-30.

15 SBA Advocacy Letter at 3.

information ("PII"),[16] which is overly-broad and consequently greatly expands the burdens imposed by other proposed requirements.

III. THE COMMISSION SHOULD NARROW THE SCOPE OF INFORMATION COVERED BY THE PROPOSED RULES

The Commission should omit the proposed rules referring to "customer PI" and apply customer proprietary network information ("CPNI").[17] Under the definition of CPNI, the sensitivity of collected information should dictate its treatment in both consumer choice and data security contexts. CCA echoes the many commenters arguing that the scope of customer PI, and hence the scope of information subject to the proposed rules, is too broad to achieve the Commission's intended goal[18] and would unduly burden all providers, but especially small and rural providers.[19] Instead, the Commission should reserve the most stringent protection rules to protect only the most sensitive data.[20]

If the Commission is wedded to adopting a form of customer PI, CCA proposes restricting the definition of PII to include only the most sensitive personal information not

---

16 *See* NPRM, Appendix A, Proposed Rule §§64.2003(h) (definition of customer PI), (o) (definition of PII), and 64.7000(g) (definition of CPNI).

17 Adopting the proposed definition of "customer PI" would violate Section 222 of the Communications Act and otherwise exceed the Commission's statutory authority. *See* CCA Comments at 13-16.

18 *See* Comments of AT&T, WC Docket No. 16-106 at 75 (filed May 27, 2016) ("AT&T Comments"); *see also* NTCA Comments at 28; Comments of FTC Consumer Protection Bureau at 9.

19 *See* CCA Comments at 11.

20 *See* CCA Comments at 11-12 (noting the proposed definitions of CPNI and PII should be limited to avoid imposing burdensome, often unnecessary requirements).

available through public means that, if released, would cause material harm to the individual.[21] Adding sensitivity and harm elements to the definition of PII would make it easier for carriers to provide more meaningful protections to consumers. This definition would also exclude publicly available information, which does not merit the same protection as sensitive information, or even information only a BIAS provider may access by virtue of their relationship with their subscriber.[22]

If the Commission will not depart from defining customer PI as encompassing both CPNI and PII, CCA cautiously supports the FTC Consumer Protection Bureau's suggestion to modify the scope of PII to include only information "reasonably" linkable to an individual subscriber.[23] If the FCC adopts the FTC's proposed definition, CCA would suggest narrowing the scope to information that is not publicly available, and would be harmful if shared. FTC explains, "[w]hile almost any piece of data could be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology."[24] This would provide a meaningful, context-based limit on information encompassed by this term, and would be consistent with other leading privacy regimes.[25] Requiring protection over information that is

---

21 *See* CCA Comments at 13.

22 *See* NTCA Comments at 28 ("[T]he Commission attempts to cast a net over data that is so pervasively public that the Commission's proposal to render it protected 'PII' sends the temperature on an already chilling shroud of regulatory disparity plummeting. In no logical world does information that is part of the public record, including physical or postal addresses, fall beneath the umbrella of protection").

23 *See* FTC Comments at 9. CCA does not support, however, tying "reasonable linkability" to devices. There are many reasons a device might not be linkable to a consumer.

24 *See* FTC Comments at 9.

25 *See* FTC Comments at 9, *citing* 5 See, e.g., 45 C.F.R. § 160.103 (defining "individually identifiable health information" in the context of the Health Insurance Portability and

"reasonably" linked to an individual consumer would be more useful for consumers by requiring providers to handle more carefully data that could actually harm that individual consumer if shared in the wrong context. Further, a customer would experience fewer, but ultimately less confusing and arbitrary, interactions with their BIAS provider for any implemented customer choice regime.[26] In any case, the Commission should strive to adopt a definition of PII that implicates a more reasonable scope of liability for the provider.

The Commission does not have to include all data conceivably related to a consumer to offer meaningful protections. Public Knowledge argues implementing an FTC-style rule that distinguishes between sensitive and non-sensitive data, or harmful data, which necessitates deep packet inspection ("DPI"). This is not practical nor reasonable.[27] By asserting "the only way to ensure those extra-sensitive communications are given adequate protection against collection and dissemination by ISPs is to assume that *all* communications could potentially contain such highly sensitive information," Public Knowledge misses the point.[28] While it is possible to glean "sensitive" aspects of an individual's life by compiling or dissecting vast quantities of data, the FCC and the FTC are responsible for ensuring BIAS providers' access to consumer data isn't

---

Accountability Act as, inter alia, information "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual").

[26] CCA does not, however, support typing "reasonable linkability" to both an individual and their devices. FTC Comments at 10.

[27] *See* Comments of Public Knowledge, WT Docket No. 16-106 at 24 (filed May 27, 2016) ("PK Comments").

[28] *See id* at 26.

abused, *not* to curb access entirely through rules that test the integrity of carriers' business models, small carriers more than others.[29]

IV. DATA SECURITY REQUIREMENTS SHOULD CONSIDER THE REASONABLE CAPABILITIES OF PROVIDERS, AND SHOULD BE GEARED TOWARD PROTECTING SENSITIVE DATA

Regarding data security, the risk management proposals are unnecessary and overly-burdensome, especially in the context of a small provider.[30] The Commission should revise its rules to focus on what kind of security and risk management measures would be "reasonable" based on the character of a provider and the context of a breach.

a. Data Security Rules Should Not Impose a Strict Liability Regime

CCA supports the FTC's suggestion that the FCC modify Section 64.7705(a) to require BIAS providers to "ensure the *reasonable* security, confidentiality, and integrity of all customer PI…"[31] The proposed rule would hold carriers strictly liable for "ensuring" the protection of data, and commenters urged the Commission to step away from this untenable approach.[32] No BIAS provider can "ensure the security… of all customer PI" and it is unreasonable to dictate

---

29 *See also* Comments of T-Mobile USA, Inc., WC Docket No. 16-106 at 5 (filed May 27, 2016) ("T-Mobile Comments") (BIAS providers degree of insight with respect to customer data is waning, as encryption becomes more ubiquitous).

30 *See id.* at 35-42.

31 FTC Comments at 27; *see also id.* ("[T]o the extent that the Commission may intend section 64.7005(b), which mentions the sensitivity of the customer information and the BIAS provider's activities, to cut back in some way on the requirements of (a), it should revise and clarify the proposed rule").

32 *See, e.g.*, CCA Comments at 37-38; *see also* FTC Comments at 27; *see also* CenturyLink Comments at 27, 35; *see also* T-Mobile Comments at 47-48.

that a provider "must" do so. The proposed rule also diminishes the "reasonable measures" approach described by Section 64.7705(b).[33]

b. The Data Security Minimums Should Be Omitted

The Commission should omit Sections 64.7005(a)(1)-(5). Prescriptive data security rules inhibit the kind of bespoke data security program carriers need to provide the best protection possible within the limits of the resources at their disposal.[34] As T-Mobile stated, "providers must be permitted and encouraged to engage in risk-based analysis [with respect to consumer harms], and to adjust protections in light of the nature and scope of their activities, the sensitivity of the data, and the size and complexity of their relevant data operations."[35] The record provides robust agreement that the proposed litany of data security requirements in Sections 64.7005(a)(1)-(5) would merely waste provider resources rather than provide meaningful security protections to subscribers.[36] Many on record agree the minimums would divert resources from being used to support network deployment, maintenance, and testing innovative new service options, all without benefitting consumers.[37]

---

33 *See* CCA Comments at 37.

34 *See* T-Mobile Comments at 48-49 ("Inevitably, minimum standards and prescriptive data security rules will inhibit providers from focusing resources on measures they deem best to protect consumers in any given circumstance, *i.e.*, reasonable measures under the circumstances").

35 *See* T-Mobile Comments at 48-49.

36 *See, e.g.*, Sprint Comments at 19 (the Commission should remove the risk management obligations because they are burdensome and targeted solely at collection and use of sensitive personal information) *see also* T-Mobile Comments at 48-49; *see also* Comments of Consumer Technology Association at 10.

37 *See* Comments of Consumer Technology Association, WC Docket No. 16-106 at 10 (filed May 27, 2016); *see also* T-Mobile Comments at 48-49.

The Commission also must acknowledge the disproportionate harm the proposed data security minimums would cause to small providers. Industry groups representing smaller providers and smaller providers themselves went to great lengths to describe the harms that these rules would inflict on the operations and budgets of small carriers, who, unable to secure cutting edge cybersecurity technology, must make strategic investments to protect the data of their subscribers.[38]

First, the proposed rule requiring risk management assessments is enormously burdensome and should be discarded.[39] Forcing small providers to provide "regular" risk management assessments "through binding regulations would be costly, time-consuming, and operationally disruptive."[40] Adding to those burdens, small providers likely would need to enlist the help of third parties to comply in any meaningful fashion, and could disrupt contracts with third parties who may not allow providers to audit their security practices.[41] As ACA noted:

> Removing this requirement will afford providers greater flexibility to determine the most effective approach to comply with the overarching requirement to protect the security, confidentiality, and integrity of customer data based on the nature and scope of the BIAS providers activities, the sensitivity of the underlying data, and technical feasibility.[42]

---

38 *See, e.g.*, WTA Comments at 18; *see also* CCA Comments at 38; *see also* ACA Comments at 23-24.

39 *See* CCA Comments at 38; *see also* ACA Comments at 23-24.

40 *See id.* at 23.

41 *See id.* at 23-24 ("To the extent these small providers use third parties to handle billing, customer service, network maintenance, security, and other functions, risk management assessments would be extremely complicated and disruptive, particularly where existing contracts do not provide for audit rights or where they prescribe data security standards different from those that the Commission proposes here. Moreover, any specific frequency requirement—e.g., one risk management assessment per year—would impose disproportionate burdens on smaller providers").

42 *See id.*

Further requiring small providers to "promptly" address any "weaknesses" detected during such assessments assumes these providers have resources to upgrade to the latest and greatest security systems, which is not accurate; this rule unfairly exposes small providers to liability. As WTA explains, "[s]mall providers do everything in their power to make sure that vulnerabilities are minimized, but they cannot be required to dedicate precious limited resources to combat a vulnerability that is not likely to be a substantial threat to the rest of the network and other services provided to their customers."[43]

Providers should not be required to designate a senior privacy official, especially small providers.[44] As ACA points out, the existing rules require small providers to designate an officer to handle CPNI compliance requirements.[45] The new rules, however, would require an individual take charge of "implementing and maintaining" those policies.[46] Small providers should not and cannot be expected to have a security and compliance expert on staff.[47]

c. The Size and Resources of a BIAS Provider Should Influence a "Reasonableness" Determination with Respect to Data Security

The Commission should modify Section 64.7705(b)(1) to provide that the size and resources of a BIAS provider shall be taken into account when determining which "reasonable"

---

43 WTA Comments at 18.

44 *See* NPRM ¶¶ 188-90.

45 *See* ACA Comments at 25.

46 NPRM Appendix A, Proposed § 64.7705(a)(3).

47 *Id.*

security measures to employ.[48] Language based on provider size and resources more clearly takes the needs of each provider into account unlike the proposed language, which addresses only the "nature and scope" of BIAS providers' activities. This is more practical than the proposed language considering a provider's size and resources are the largest predictors of what kind of data security safeguards can actually be implemented, based on budget, or should, based on the best option budgeted resources can afford. Consumers would not be harmed by CCA's suggestion, considering Section 64.7705(b)(2)[49] would remain undisturbed.

d. A "Best Practices" Regime Should be Avoided

CCA generally supports the creation of a best practices regime,[50] but does not support the use of any regime as a codified rule applicable to all BIAS providers. If the Commission does adopt a "best practices" regime, they should be mindful that even adhering to a "best practices" regime may not be applicable or reasonable for the smallest carriers, nor is it necessary to protect their consumers. CSRIC has acknowledged that small and medium-sized businesses face unique constraints that may impact their ability to adhere to a complex "best practices" framework in all circumstances.[51] Small providers are often not included in the creation of "best practices"

---

48 *See* RWA Comments at 10 (if the Commission does ultimately codify a security requirement, it should take a BIAS provider's size and resources into consideration, and further apply a reasonability standard); *see also* ACA Comments at iv.

49 Requiring a BIAS provider to take into account the "sensitivity of the [customer PI] held by the BIAS provider."

50 *See* CCA Comments at 34-35.

51 *See* ACA Comments at 23, *citing* the Communications Security, Reliability and Interoperability Council IV, Working Group 4, Final Report, 25, 375 (Mar. 2015) ("As the Communications Security, Reliability and Interoperability Council (CSRIC) recognized in its 2015 Working Group Four Final Report, 'Small and Medium Businesses (SMBs) have unique circumstances and challenges that may influence their approach to implementing the [NIST Cybersecurity]

regimes, and therefore the unique needs of these parties are not likely to be included in the final set of best practices. Further, best practices regimes tend to be more frequently updated than federal regulations and could present a "moving target" for BIAS providers. Accordingly, the Commission should resist encoding perceived "best practices," as such regimes are still developing and are not always reasonably attainable for small providers.[52]

V. DATA BREACH RULES SHOULD BE DESIGNED TO ENSURE A "REASONABLE" RESPONSE

The Commission should modify the data security rules to reflect a more meaningful definition of "breach," calibrate requirements to send data breach notices with the sensitivity of the underlying data, and relax other prescriptive data notification rules as described below.

a. Definition of Breach Should Include an Intent Component, and Other Context-Based Qualifiers

The Commission should redraft the proposed definition of "breach" provided in Section 64.2003(d) to include qualifiers such as "the potential size of the breach, the elements of intent and/or harm, and the sensitivity of the data at issue, or some combination of these qualifiers."[53] As noted on record, it is nonsensical for the Commission to promulgate a rule wherein "even unintentional breaches causing no consumer harm would trigger notification obligations…As a result, the proposed rules would dramatically expand the situations in which a breach notification

---

Framework and providing macro-level assurances," and "there is no one-size fits all approach to cybersecurity risk management").

[52] *See* CCA Comments at 41 (FCC's proposed data security requirements may even quell the natural progression of data security best practices currently being developed).

[53] Sprint Comments at 15; *see also id.* at 16 ("Sprint believes that customers would be best served by notice when there is a risk of harm (including whether the breach involved the disclosure of sensitive data) or misuse").

would be required, increasing the total costs of compliance, as well as the risk of costly enforcement actions."[54]

Without an intent element or other qualifiers connecting a required response to the character of the "breached" data, the FCC would create an over-notification problem. This will seriously jeopardize consumer welfare.[55] The FTC notes the danger of consumers becoming desensitized to a "barrage of notices," which means consumers could "become numb to such notices, so that they may fail to spot or mitigate the risks being communicated to them."[56] Worse, any notices sent by BIAS providers will arrive on top of other breach notifications by parties under different regimes, and FTC references data indicating consumers may already be overwhelmed by the volume of breach notices they receive.[57] Considering the scope of information covered, consumers will be confused as to whether a data breach is truly a danger to their well-being. This policy does not benefit consumers and should not be codified.

An accidental data breach by an employee, for example, should not trigger a notice, nor should nefarious access to encrypted data. Under these circumstances, there is no reasonable risk to the consumer, and no action the consumer can take to ameliorate the situation. In sum, "Any breach notification requirement must account for when consumers actually are put at risk and when they were not."[58]

---

54 ACA Comments at 35; *see* T-Mobile Comments at 51.

55 *See* T-Mobile Comments at 50 ("Overnotification will mute the value of transparency and engender consumer confusion"); *see also* FTC Comments at 31-32; *see also* CTIA Comments at 176-177.

56 FTC Comments at 31.

57 *See* FTC Comments at 32.

58 *See* T-Mobile Comments at 51.

b. Data Breach Rules Should Be Context-Based Under a Reasonable Notification Timeframe

The Commission should revise the notification rules encoded under Section 64.2006 to allow providers more flexibility and more time to respond to a data breach. As described on record, forcing carriers to run through a long and onerous compliance checklist in the midst of a security incident actually increases the likelihood of consumer harm. Instead of, for example, trying to cut off a botnet or enlisting the services of a data security firm, a carrier would have to busy itself with compiling a detailed list of information related to the breach including "a description of the customer PI that was disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed…"[59] This information may not even be known to carriers at the time of a breach.[60] Further, the Commission should not require a separate report in the event a telecommunications service provider discovers a breach that they reasonably believe has affected at least 5,000 customers. If it does enact this rule, the Commission should limit completion and submission of one form so time is not wasted filling out duplicative paperwork.[61]

The cost of complying with breach notification rules would be too expensive for small providers, and unduly burdensome for other carriers. As provided in the record, the notification costs associated with a data breach can extend well beyond $130 per person.[62] That adds up

---

59 *See* NPRM Appendix A, Proposed Rule § 64.2006(a)(2)(ii); *see also* T-Mobile Comments at 54 (the current notification timeline threatens to imperil consumers by diverting important BIAS company resources to complying with Commission rules rather than addressing the damage caused by the breach).

60 *Id.*

61 *See* Comments of Verizon, WC Docket No. 16-106 at 70 (filed May 27, 2016).

62 *See* ACA Comments at 35, *citing* Draft NISTIR 7621 Revision 1, *Small Business Information Security: The Fundamentals,* Richard Kissel, Hyunjeong Moon, U.S. Department of Commerce,

quickly. A breach involving 1,000 customers whose data was or might have been compromised in an incident could result in a $130,000 per incident price tag.[63] This metric alone supports a more expansive small provider exemption.

At the outset, the proposed notice timeline is unreasonable.[64] Commenters were particularly outspoken on this issue.[65] The Commission should adopt the FTC's "without unreasonable delay" standard, with a reporting ceiling of between 30 and 60 days.[66] The proposed data breach timeline and requirements "could potentially leave providers with an impossible choice – either ignore what consumers may need post-breach or divert resources to such efforts rather than to the investigation of the breach."[67] The FTC's recommended timeline "would be adequate for companies while protecting consumers."[68] A lighter requirement, such as an "as soon as practicable" standard, would be justified, especially for small providers.[69]

VI. CUSTOMER CHOICE FRAMEWORK

CCA opposes the proposed customer choice framework provided by Section 64.7002; the Commission should adopt an opt-out only regime, based on the sensitivity of the information

---

2 (December 2014) ("The average estimated cost for these notifications and associated security breach costs is well over $130 per person").

63 *Id.*

64 *See* NPRM, Proposed Rule §§ 64.2011, 64.7006.

65 *See* T-Mobile Comments at 53; *see also* FTC Comments at 34; *see also* WTA Comments at 13; *see also* ACA Comments at 46; *see also* Sprint Comments at 16-18; *see also* NTCA Comments at 67; *see also* CTIA Comments at 175-178; *see also* FTC Comments at 34.

66 *See* FTC Comments at 34.

67 *See* T-Mobile Comments at 54.

68 *See* FTC Comments at 34.

69 *See* WTA Comments at 13.

shared.[70] Any opt-in/opt-out framework, however, should operate to afford the highest protections to only sensitive data.

a. Opt-In Consent, If Adopted, Should Be Used Only for Sensitive Information Collected By BIAS Providers

If the Commission adopts an "opt-in" component, Section 64.7002(f) should be revised to require opt-in consent only where a BIAS provider wishes to share, use or disclose sensitive information, including (1) content of communications[71] and (2) Social Security numbers and children's, financial, health, or precise geolocation data.[72] In all other cases where consent is not inferred, an opt-out requirement will afford adequate consumer protection. CCA also believes rules impacting how information is shared, used, or stored should revolve around the sensitivity of the data, which protects consumers by taking into account the "different expectations and concerns that consumers have for sensitive and non-sensitive data."[73]

---

70 *See* CCA Comments at 22 ("The expansive opt-in/opt-out regime proposed by the FCC is not narrowly tailored to the goal of protecting consumer information, and must be rejected"); *see also* T-Mobile Comments at 27 (the successful "opt-out" regime that has protected customers across the Internet should be adopted; opt-out framework has "prompted the development of innovative new services that benefit consumers," without compromising meaningful control over data).

71 "The term 'content' includes consumer communications such as contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, movies watched – all of which applies whether a consumer uses a traditional computer or an Internet-connected device." FTC Comments at 20.

72 *See* FTC Comments at 20; *see also* FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers* at 55-56 (Mar. 2012), *available at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers ("Privacy Report"); *see also* Comments of the Internet Commerce Coalition, WC Docket No. 16-106 at 10 (filed May 27, 2016) ("Internet Commerce Coalition Comments") (The most onerous rules, like opt-in, should be reserved for only the most sensitive data, like Social Security numbers and children's, financial, health, and geolocation data).

73 FTC Comments at 22.

CCA also agrees with the FTC that the Commission's proposed rules "could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful."[74] Many T-Mobile subscribers enrolled in *Binge On*,[75] for example, would likely welcome an updated list of *Binge On* partners in their inbox with targeted recommendations. On the other hand, a consumer would be understandably upset or confused if, after paying for a certain brand medication online, they suddenly received an email from their BIAS provider offering coupons from a competing pharmaceuticals company.

Research supports that the FTC's suggested parameters meet consumer expectations.[76] Even as 91% of adults indeed agree or strongly agree that consumers have lost control of how personal information is collected, "most Americans who are making decisions about sharing their information in return for a product, service or other benefit" say "the context and conditions of the transactions" dictate their decisions, including the "terms of the deal; the circumstances of their lives; whether they consider the company or organization involved to be trustworthy; [and] what happens to their data after they are collected."[77] For example, 90% of adults consider Social Security numbers to be "very sensitive," and 50% of adults also consider information about their health and medications, the content of their email and phone conversations, or details

---

74 *Id*.

75 *Binge On* is a free incentive that enables T-Mobile customers on a qualifying Simple Choice plan to stream unlimited 480p video from dozens of partnered services, including Netflix, HBO NOW, Hulu, and YouTube, without any of the data consumed counting towards their plans.

76 *See* Lee Raine, *The state of privacy in America; What we learned*, PEW RESEARCH CENTER (Jan. 20, 2016), *available at* http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

77 *Id.*

of their "physical location over time" to be "very sensitive."[78] On the other hand, only 8% found information about "basic purchasing habits" to be "very sensitive."[79] Research therefore shows different information draws different degrees of concern; consumers are not, as the FCC's proposed rules seem to reflect, worried about *all* of their online data, and context matters. Further, the record reflects consumers want BIAS providers to use their data in useful ways.[80]

CCA disagrees that rules based on sensitivity would result in a less predictable or straightforward approach.[81] Paul Ohm submitted that "if customers were protected by an opt-in rule for sensitive information alone, Comcast, AT&T, Time Warner, Verizon, etc., would each come up with its own definition…"[82] To follow the example, it would appear slight variations in a definition of "sensitive" would not cause material harm to consumers as long as they are anchored in affording greater protection to those categories outlined by the FTC: customer content and information with the same sensitivity as Social Security numbers and children's, financial, health, or precise geolocation data. Flexibility is beneficial in this context, as definitions and consumer expectations will change as broadband-based technology itself develops. Broadband technology simply does not lend itself well to "bright line" categorizations. Furthermore, it does not seem the FCC would struggle to assert authority over a

---

78 *Id.*

79 *Id.*

80 *See, infra, Section IV.b.*

81 *See* Reply Comments of Paul Ohm, WC Docket No. 16-106 at 6-10 (filed June 22, 2016) ("Paul Ohm Comments").

82 Paul Ohm Comments at 12.

data-gathering or sharing practice that offends its principles.[83] The parameters offered by the FTC draw meaningful lines that will guard consumers' most important information. The Commission should not feel compelled to adopt a rule encompassing all information, and should delineate between sensitive and non-sensitive data.

b. The Commission Should Embrace a "Total Service Approach" For First Party Marketing of "Additional BIAS Offerings in the Same Category of Service"

The Commission should apply a "total service approach" [84] to broadband and, as FTC has recommended, refrain from designating certain practices for which consent is implied;[85] this would allow carriers to engage in higher quality first party marketing for which consent is inferred under proposed Section 64.7002(b). The Commission should, considering the broad and growing array of mobile applications available, resist subscribing subcategories of services qualifying as "additional BIAS offerings in the same category of service (e.g., fixed or mobile BIAS)."

---

83 *See, infra,* Section III; *see also See Cellco Partnership, d/b/a Verizon Wireless,* Order & Consent Decree, File No.: EB-TCD-14-00017601, *et al.*, DA 16-242, at 6-10 (rel. Mar. 7, 2016).

84 Current CPNI rules allow carriers "to use a customer's entire record, derived from complete service subscribed to from that carrier, to market improved services within the parameters of the existing customer-carrier relationship" and "permits carriers to use CPNI to market offerings related to the customer's existing service to which the customer presently subscribes." *See Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, ¶ 16 (rel. Aug. 16, 1998). The Commission has since affirmed that "[b]ased on the language of section 222(c)(1), Congress intended that a carrier could use CPNI without customer approval, but could only do so depending on the service(s) to which the customer subscribes. The total service approach defines the parameters of those services and thus defines what carriers may do without the approval of the customer." *Implementation of the Telecommunications Act of 1996*, Third Report and Order and Third Further Notice of Proposed Rulemaking, FCC 02-214, ¶¶ 83-84 (2002).

85 *See* FTC Comments at 15.

Public Knowledge argues that "the proliferation of IP-based services has opened up numerous attempts at regulatory arbitrage" where a "total service" approach is concerned with respect to first party marketing. Public Knowledge further argues that "[a]pplying the total service approach to broadband services would run directly against consumer expectations, as it would open the door to their 'implied consent' being used to market products that do not meet their expectations of 'broadband services.'" It is doubtful Public Knowledge can substantiate the idea that consumer expectations for what constitutes "broadband services" is not greatly expanded, considering broadband services touch nearly every aspect of daily life: healthcare, automobiles, banking, entertainment, and interacting with one's social network. This is not "regulatory arbitrage;" it's the way broadband technology has evolved, and will continue to evolve.

Treating BIAS providers as public utilities simply responsible for turning a resource on or off severely underestimates the role that broadband providers, particularly mobile providers, have assumed in American society, and the myriad benefits they provide. Public Knowledge argues that "the Commission must not draw a definition [of BIAS services] so broad as to include directional service offerings such as music or video streaming or other 'walled gardens' that providers could offer in lieu of obtaining the required opt-in consent for similar non-IP-based services."[86] On the contrary, CCA asserts "additional BIAS offerings in the same category of service" *should* encompass services like music or streaming video. In 2015, total mobile wireless subscriber connections neared an all-time high of 370 million.[87] Annual data traffic has

---

86 PK Comments at 31.

87 *See* CTIA-The Wireless Association, CTIA's Wireless Industry Summary Report, Year-End 2015 Results (2015).

tripled since 2013.[88] It is clear subscribers want (and, in some commercial or economic contexts, need) certain network speeds, resolutions, and capabilities. Consumers preform increasingly sophisticated work and play on their mobile devices. The Commission therefore needs to remove barriers to implementing these new technologies, not attempt to thwart their proliferation.

The FCC should not pretend zero-rated services, enhanced streaming video or music platforms, and other data-cap-oriented or package deals are not an expected part of the mobile broadband experience. Sprint explains that "[c]onsumers today fully expect, and increasingly *demand* that the companies with which they share their personal information will use that data to market new and relevant services to them."[89] CCA agrees with CTIA that consumers would not be surprised to receive such service offerings, given their "general understanding of the Internet and the services offered by their Internet service providers ("ISPs"), and the prevalence of bundled offerings that extend beyond access services to include value-added content and other features."[90]

---

88 *See id.*

89 Sprint Comments at 9, citing Peter Dahlstrom & David Edelman, *The Coming Era of 'On-Demand' Marketing*, MCKINSEY QUARTERLY (Apr. 2013), *available at* http://www.mckinsey.com/business-functions/marketing-and-sales/ourinsights/the-coming-era-of-on-demand-marketing (forecasting increase in customer "expect[ations] [that] all data stored about them [will] be targeted precisely to their needs or used to personalize what they experience."); *see also* Sprint Comments at 21 ("Indeed, evidence increasingly shows that consumers willingly disclose such information to obtain a variety of benefits, including personalization, free services, and useful advertisements").

90 *See* CTIA Comments at 124.

There is support in the record showing all providers, small providers included,[91] should be able to "effectively market and deploy innovative products to their consumers," as "more customers expect their BIAS providers to offer these value-added services—and choose their BIAS provider based on those services."[92] The FCC should facilitate access to technologies consumers desire.

c. The "Dashboard" Provisions Should Be Eliminated

The Commission should omit proposed Section 64.7002(d) and otherwise relieve providers, especially small providers, from the need to implement any "customer dashboard"[93] interface to comply with notice and choice regulations.[94] As NTCA notes, the proposed "dashboard" would require "both initial design, coding, and on-going updates to user's on-line profiles. [It would be] an extraordinarily complex exercise to capture all individual variables and to convey them meaningfully to every consumer,"[95] and would be extremely difficult if not impossible for small providers to accomplish. WTA notes small providers lacking online portals and/or web development staff would have to engage a third-party to develop a dashboard.[96] To

---

91 *See* ACA Comments at 41; *see also* CCA Comments at 25 ("CCA members seeking to effectively compete with larger carriers should not be limited to only marketing existing services").

92 ACA Comments at 41.

93 *See* NPRM ¶ 95 (seeking comment on the burdens of a consumer-facing privacy dashboard).

94 *See* Sprint Comments at 13-14; *see also* ACA Comments at 39; *see also* NTCA Comments at 42; *see also* WTA Comments at 10-11; *see also* Comments of Electronic Frontier Foundation, EC Docket No. 16-106 at 13-14 (filed May 27, 2016); *see also* CTIA Comments at 104.

95 NTCA Comments at 42

96 *See* WTA Comments at 10-11 ("[M]any small providers do not currently have online portals through which consumers may change their privacy preferences and lack web development staff that would make development of such a tool more affordable and practicable").

make matters worse, under the proposed rules this third party involvement would likely implicate additional costly oversight or contractual burdens. The Electronic Frontier Foundation ("EFF") recognizes the enormous burden the dashboard would create for small providers, and encourages the Commission to consider alternatives.[97] The Commission should allow providers the flexibility to design their own notice policies, as long as they are "sufficiently prominent, effective, and easy to use."[98]

Moreover, the record reflects that small carriers are unlikely to successfully absorb burdens stemming from the customer choice framework, taken as a whole. In its comments, CCA explained in detail how the customer choice framework disproportionately impacts small and medium-sized carriers.[99] Others representing small and rural carriers made similar observations. For example, ACA discussed how increased legal fees following promulgation of an opt in/opt out framework would harm providers, noting that "small providers would need the help of a specialist, likely an attorney, to ensure services are property categorized (i.e., "communications-related" or not) and determining whether opt-in or opt-out applies."[100] The cost of implementing the proposed customer choice framework to small carriers alone, as noted on record, would "foreclose the ability of small providers to defray the cost of deployment and ongoing investment."[101] The detailed, extensive support on this subject throughout the record surely justifies a revision of the proposed rules to address small provider harms.

---

97 *See* EFF Comments at 13-14.

98 *Id*.

99 *See, e.g.*, CCA Comments at 18.

100 *See* ACA Comments at 30.

101 WTA Comments at 14.

VII. THE FCC'S PROPOSED REGULATIONS WILL BE ILL-RECEIVED BY CONSUMERS AND WILL DISCOURAGE COMPETITION IN THE TELECOMMUNICATIONS MARKETPLACE

a. The Proposed Rules Will Confuse and Aggravate Consumers

There is robust support in the record that the proposed rules would confuse, rather than protect, consumers.[102] The dangers of over-notification "are not mere speculation; they find support from scientific studies, which demonstrate that consumers are not served by expansive, untimely, and repetitious privacy notices."[103] Further, consumers are unlikely to distinguish between Internet actors in the context of actual Internet use, therefore the rules in the NPRM would generate confusion about what information is protected, and under which particular regime.[104] For example, a user who declines an opt-in notice from her BIAS provider to receive

---

102 *See* NTCA Comments at 11; *see also* AT&T Comments at 57; *see also* CTIA Comments at 153; *see also* T-Mobile Comments at 29.

103 CTIA Comments at 100, *citing* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & Pol'y for the Info. Soc'y 543 (2008) (calculating the high costs of time spent reading privacy notices and suggesting that both the frequency and length of privacy policies are problematic); *cf.* Edith Ramirez, Chairwoman, FTC, *Privacy and the IoT: Navigating Policy Issues* 7, Opening Remarks at International Consumer Electronics Show (Jan. 6, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf (noting that "we risk inundating consumers with too many choices," and advocating a simplified approach); FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* 18 (Feb. 2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-throughtransparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (noting that the importance of ensuring that information does not become "too complex to be useful to consumers").

104 *See* AT&T Comments at 57; *see also* T-Mobile Comments at 29 ("[C]onsumers do not expect that their broadband provider operates in a different manner as providers of other Internet services with respect to how their information is used and disclosed. Thus, consumers do not, and would not, expect to provide opt-in consent for uses of their non-sensitive information"); *see also* CTIA Comments at 153 ("There is no reason a consumer would expect that online security or data practices will vary dramatically, with ISPs being subject, for example, to detailed authentication obligations or prohibitions on data collection, while social media companies are not. It will be difficult for consumers to appreciate the difference between ISPs and edge providers enough to

updates from a media partnership with ESPN may nonetheless receive ESPN-targeted ads based on the user's actions on social media platforms tracking their preferences. The user in this scenario might think the provider had not respected the user's opt-in choice, unduly harming their relationship with their BIAS provider. There are a wealth of other examples in the record that should persuade the Commission to seriously reconsider the imposition of a confusing, inconsistent regime.[105]

b. The Commission Should Adopt the Industry Proposal, Which Protects Consumers Without Sacrificing BIAS Provider Competitiveness

The Commission should adopt privacy and data security rules articulated in the Industry Proposal. The Industry Proposal protects consumers without compromising the business needs of BIAS providers or sacrificing provider competitiveness in the marketplace. Further, the Industry Proposal is consistent with the regime regulating privacy across all non-BIAS participants in the online economy. In this respect especially, it promotes consumer welfare by making it easier for consumers to understand the scope of their choices regarding how their information is shared, used, or stored.

Many parties recognized the value of regulating all sectors taking part in the Internet ecosystem on a consistent basis, and the importance of putting all competitors on an "equal playing field."[106] As the FTC noted, an outcome whereby "FCC's proposed rules, if implemented, would impose a number of specific requirements on the provision of BIAS

---

understand that one could only hold data for a certain amount of time, while the other has no such limitations").

105 *See, e.g.*, CTIA Comments at 127-136.

106 *See, e.g.*, NTCA Comments at 8-10 ("with a broad roster of broadband players, a uniform set of standards creates a level playing field and rational set of consumer expectations").

services that would not generally apply to other services that collect and use significant amounts of consumer data…is not optimal."[107] CCA notes that some parties traditionally outside the telecommunications industry appear to underestimate the scope of the Commission's proposed rules. Mozilla, for example, expresses general support for the NPRM because it is "consistent with best practices in our industry."[108] While this may be true, these best practices should be applied equally throughout the industry for a truly consistent approach. Edge providers as yet are not micromanaged under rules comparable to those in the NPRM, and are not, for example, facing down the prospect of assuming liability (rather, "ensuring" protection) when storing data or sharing data with partners and affiliates, coupled with a duty to police the conduct of those parties. The FCC is creating a patchwork of privacy rules that are confusing at best and anti-competitive at worst, by giving a significant competitive advantage to one segment of the industry.

The Internet economy demonstrates the need for flexibility with respect to privacy notice and disclosure, depending on a providers' service offerings and development strategy. NTCA discussed the myriad of data collection practices of major edge providers like Google, who "has introduced new artificial intelligence (AI) software that will analyze the content of text messages and photos in order to recommend responses to received messages; the software will also 'learn' user preferences in order to provide tailored responses to inquiries. Amazon, Facebook, WhatsApp, and Apple offer competing technologies. The Washington Post uses cookies, web

---

107 FTC Comments at 8; *see also id.* ("FTC staff continues to believe that such generally applicable laws are needed to ensure appropriate protections for consumers' privacy and data security across the marketplace").

108 Mozilla Comments at 6.

beacons and 'other technologies' for online tracking and advertising."[109] Apple recently began using "differential privacy" technology, which is designed to show engineers "patterns on how multiple users are using their devices," allowing insight as to "how customers are using [for example] emojis or new slang expressions on the phone, or which search queries should pop up 'deep links' to apps rather than webpages."[110] This is considered something of a leap for Apple, whose privacy policy always has explicitly centered on selling hardware and refraining from mining individual data. Nonetheless, in efforts to keep up with advances in machine learning led by Google and other businesses with more aggressive data mining policies, Apple is free to experiment with a less invasive privacy practice that might very well advance its machine learning capacity and improve its products. While these practices certainly implicate privacy concerns, the promise of consumer benefits is even more tangible. Providers who are transparent about their practices, and are not using that data in harmful ways, should have regulatory space to innovate.

Chairman Wheeler recently stated "American leadership in 5G should be a national priority. The driving force of the 21st century will be powerful processing centralized in the cloud and wirelessly connected."[111] Indeed, despite the consolidated nature of the market and the lack of competition for critical mobile inputs, the wireless industry generates a "significant

---

109 NTCA at 8-10.

110 *Id.*

111 Prepared Remarks of FCC Chairman Tom Wheeler, *The Future of Wireless: A Vision for U.S. Leadership in a 5G World*, National Press Club, Washington, D.C. (June 20, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0620/DOC-339920A1.pdf ("Chairman Wheeler *Future of Wireless* Remarks").

economic activity and creates a large footprint on the U.S. economy."[112] The wireless industry is not perfect, but it is profitable.[113] Further, the U.S. is in the enviable position of global leader with respect to mobile broadband. The U.S. leads in LTE deployment, and has 50 percent of the world's 4G subscribers despite claiming less than 5 percent of global wireless subscribers.[114] Considering, as Chairman Wheeler has remarked, ""[a]utonomous vehicles will be controlled in the cloud[,][s]mart-city energy grids, transportation networks, and water systems will be controlled in the cloud[, and i]mmersive education and entertainment will come from the cloud,"[115] with the right policies, wireless broadband providers are poised to make even bigger contributions to the American and international economy.

If the Commission is determined to "stay out of the way of technological development,"[116] they should not impose privacy rules that impede economic progress without

---

112 The Brattle Group, *Mobile Broadband Spectrum: A Vital Resource for the U.S. Economy* (May 11, 2015), *available at* http://www.ctia.org/docs/default-source/default-document-library/brattle_spectrum_051115.pdf ("Brattle Group Study"); *see also* Deloitte, *The Impact of 4G Technology on Commercial Interactions, Economic Growth, and U.S. Competitiveness* (August 2011), *available at* http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-impactof4g-101914.pdf ("Deloitte Study") ("U.S. Investment in 4G networks could fall in the range of $25–$53 billion during 2012–2016; conservatively, these investments could account for $73–$151 billion in GDP growth and 371,000–771,000 new jobs").

113 The wireless industry supported approximately $400 billion in spending and over 1.3 million jobs in the U.S. in 2013. *See* Brattle Group Study at 19. Spending by the wireless industry flowing through the economy contributed about $200 billion to U.S. GDP. *See id.* This value-add produced by the wireless industry comprised approximately 1 percent of the $16.7 trillion U.S. GDP in 2013. *See id.* The wireless industry also "directly paid over $18.4 billion in federal taxes and $23.8 billion in state and local taxes in 2013." *Id.*

114 *See* Deloitte Study.

115 Chairman Wheeler *Future of Wireless* Remarks.

116 *Id.*

demonstrable benefits to consumers. Digital advertising and innovative data management applications represent amazing technological innovations. To be sure, the proposed rules, as presented, would seriously chill the ability of BIAS providers to participate in the digital advertising marketplace. This gives a clear competitive advantage to edge providers. At present, the 59.6 billion dollar digital advertising market is dominated by Google, Facebook, Yahoo, Microsoft and Twitter, whom together account for 65% of all revenue from digital advertising in 2015, or $38.5 billion out of $59.6 billion.[117] These businesses, however, are regulated by the FTC and therefore may operate more flexibly. The FCC cannot ignore that mobile has a role to play. Although largely from the dominant providers, mobile now accounts for more than half of all digital advertising spending.[118] CCA urges the Commission to provide a set of rules that protects consumers without seriously handicapping BIAS providers hoping to compete against the likes of Google and Facebook in the digital advertising marketplace.

If the Commission wants to keep its "homefield advantage," mobile providers should not be left out of the booming Internet of Things ("IoT") marketplace, either, which will grow more ubiquitous as small cell and 5G network deployment accelerates.[119] 5G networks,[120] as many have acknowledged in the context of IoT, Business Data Services ("BDS"), and Spectrum Frontiers, will by their very nature involve more data generation and sharing. IoT technologies

---

117 Kristine Lu & Jesse Holcomb, *Digital News Revue: Fact* Sheet, PEW RESEARCH CENTER, *available at* http://www.journalism.org/2016/06/15/digital-news-revenue-fact-sheet/.

118 *Id.*

119 Chairman Wheeler *Future of Wireless* Remarks.

120 *See* See Young Lee & Miyoung Kim, *Samsung Electronics best on 5G to jump-start networks business*, REUTERS (June 21, 2016), *available at* http://www.reuters.com/article/us-samsung-elec-5g-idUSKCN0Z70KW (Samsung is targeting more than 10 trillion won ($8.6 billion) in annual sales of 5G equipment by 2022).

are poised to provide myriad benefits to society. For example, bulk data analysis of information collected from connected health devices "can facilitate health research and lead to breakthroughs in treatment.[121] Similarly, analysis of data collected from a connected public infrastructure to detect, for example, the lighting patterns on public streets, can help improve energy efficiency."[122] IoT-driven analysis of aggregated data facilitate breakthroughs in healthcare, public infrastructure, and energy efficiency, but "can also help target public service messages and resources to relevant populations, including low-income and disadvantaged communities."[123] In this context, many commenters rightly have acknowledged concerns for consumer vulnerabilities, and about unethical uses of such data.[124] Notice and choice play an important role in IoT, but CCA agrees with the FTC that there is no "one-size-fits-all approach" with respect to providing choice.[125] Implementing flexible, forward-looking privacy rules will foster

---

121 *See, e.g.*, C Spire Telehealth, White Paper (2015) (C Spire uses high speed connectivity to enable telehealth throughout Mississippi. C Spire's partnership with the University of Mississippi Medical Center (UMMC) and Intel-GE Care Innovations to provide people with diabetes more consistent and timely access to clinicians through the use of telehealth technology in their homes).

122 Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning, Docket No. 160331306-6306-01 at 4 (June 2016), *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf?utm_source=govdelivery ("FTC IoT Comments") (FTC's comments before the Department of Commerce National Telecommunications & Information Administration Request for Comment titled *In the Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*).

123 *Id.*

124 *See id.* at 6-7 ("In addition to the volume of data that can be collected by a single IoT device, the ability to link and associate multiple IoT devices to the same user can also pose material privacy r isks").

125 *See id.* at 12.

competition between edge providers and BIAS providers while ensuring customers continue to control their sensitive data.

VIII. NOTICE AND TRANSPARENCY

CCA joins others on record encouraging the Commission to re-draft Section 64.7001 to offer general guidelines for flexible privacy notices, rather than to require a rigid template.[126]

a. Rules For Notice of Privacy Policies Should Not Be Overly-Prescriptive

CCA agrees that any notices should be "clear and conspicuous," "comprehensible," and "legible."[127] These rules should be harmonized across both voice and data, so as to avoid greater compliance burdens and customer confusion.[128]

Regarding disclosures of choices available to the consumer with respect to data sharing, CCA agrees with others on record that providers should be allowed to provide notice of different choices within the governing customer agreement or privacy policy, rather than a standalone document, and allow ISPs to make privacy policy updates available through links on provider websites.[129] This makes sense, as "any broadband customer, by definition, has the capacity to receive electronic notifications."[130]

---

126 *See id.* at 9-10; *see also* Sprint Comments at 12 ("Sprint urges the Commission to give BIAS providers the flexibility to design and choose the most effective privacy notice to educate consumers within the user experience"); *see also* CTIA Comments at 98-101.

127 NPRM, Proposed Rule § 64.7001.

128 *See* WTA Comments at 13.

129 *See, e.g.*, CTIA Comments at 98-101.

130 *Id.* at 102; *see also* Sprint Comments at 12 ("[T]he Commission should confirm that BIAS providers can provide a point-of-sale privacy notice as part of the customer agreement, rather than as a standalone document. Customers receive a significant amount of information at the point-of sale").

The Commission should refrain from adopting new notice and disclosure rules for privacy with respect to small providers, considering disclosure requirements set forth in the *2015 Open Internet Order* adequately protect consumers[131] and any new rules may be contradictory and confusing. Many CCA members already provide subscribers with a clear picture of their privacy policies on their monthly bill or by annual notice, and maintain a website with their privacy policies described as required by the *2015 Open Internet Order*.[132] The Commission should refocus its efforts on holding carriers to the promises they make within public-facing privacy policies, and whether those policies are accurately expressed. This would afford consumers far better protection than developing a prescriptive formatting rule.[133]

b. Providers Should Be Allowed to Choose How Consumers Receive Advance Notice of Material Changes to Privacy Policies

If the Commission decides providers are required to provide advance notice of material changes in privacy policies,[134] providers should be able to determine how. For example, clear notice on a monthly bill would be sufficient to alert customers to any pending privacy policy changes. Again, CCA reminds the Commission that any advanced notification requirements must consider the practices, operations and limitations of small and non-nationwide mobile

---

131 *See* CCA Comments at 18; *see also* 2015 Open Internet Order, *see also Preserving the Open Internet*, GN Docket No., 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905 (2010) ("*2010 Open Internet Order*"), *aff'd in relevant part Verizon v. FCC,* 740 F.3d 623 (D.C. Cir. 2014).

132 *See* Comments of CCA at 17.

133 *See* Comments of Cincinnati Bell Telephone Company LLC, WC Docket No. 16-106 at 12 (filed May 27, 2016) (supports telecommunications service providers' adopting their own privacy policies, describing what information they collect, how they will use it, and whether and how it will be shared with third parties – this conduct should then be judged by their adherence to their stated privacy polices).

134 *See* NPRM Appendix A, Proposed § 64.7001(c).

BIAS providers.[135] As NTCA points out, "notice of the change provided by electronic means to the consumer, i.e., via email and in a billing statement, is sufficient, and that the notices then available at the firm's website can be relied upon to provide sufficient information to the customer."[136]

c. The Commission Should Adopt An Exemption For the Use, Disclosure, or Access to Information of Non-Residential Customers.

In addition to the changes proposed above, CCA would support an exemption for BIAS provider use, disclosure of, or permitting access to, information of non-residential business customers, as mentioned by others in the record.[137] The privacy needs of non-residential business customers are quite different than the monthly individual subscriber clearly envisioned by the NPRM. CTIA correctly notes there is precedent for such an exemption and the Commission should follow it.[138]

IX. THIRD PARTIES

The Commission should refrain from imposing prescriptive responsibilities for dealings with third parties in a data security context and under the proposed customer choice

---

135 *See* CCA Comments at 20.

136 NTCA Comments at 42.

137 CTIA Comments at 142 (the FCC adopt a specific exemption for ISP use or disclosure of, or permitting access to, the information of non-residential customers (*i.e.*, business customers)); *see also* Comments of INCOMPAS, WC Docket No. 16-106 at 4 (filed May 27, 2016) (the Commission should consider additional flexibility of section 222 obligations for business customers under the "business customer exemption," and CPNI rules should be modified so business customers who can negotiate for the services themselves).

138 *See* CTIA Comments at 82; *see id.* at 142, *citing* 47 C.F.R.§ 64.2010(g).

framework.[139] Oversight over third parties is unrealistic for any carrier.[140] Small carriers in particular are not be able to dictate contractual privacy terms to the extent the FCC deems necessary.[141] The Commission should evaluate providers on the protections they themselves are "reasonably" capable of providing, which may mean something different for a small carrier versus a large carrier. Regardless, actionable liability should not attach to a provider when a third party errors.[142]

With respect to working with device manufacturers, for example, CTIA notes that "ISPs are also not in a position to demand or ensure compliance by entities like device manufacturers and operating system providers. In a world in which the Commission wants consumers to be able to choose their own devices, it is clear that ISPs do not control the design and maintenance

---

139 *See, e.g.*, NPRM ¶¶ 161-62, 151 (proposal to require BIAS providers to contractually prohibit third parties receiving aggregate customer data from re-identifying received information, and to monitor those entities' compliance); *see also id.* at ¶ 212 (suggesting BIAS providers should ensure third parties protect consumer data by obtaining contractual commitments from third parties to safeguard that data, seeking comment on what precise contractual terms should be required); *see also id.* at ¶ 213 (seeking comment as to whether FCC should require mobile BIAS providers to "use their contractual relationship with mobile device or mobile operating system (OS) manufacturers" to obtain contractual commitments to safeguard shared data); *see also id.* at ¶ 255 (contemplating requiring BIAS providers to contractually require third parties with which they share customer PI to follow the sale breach notification rules proposed in the NPRM); *see also* ACA at 27 (recognizing the NPRM implies providers might have to "pass through [proposed] data security requirements to third parties by contract).

140 *See* ACA Comments at 27-28.

141 *See* RWA Comments at 12-13; *see also* CTIA Comments at 166 ("[H]olding ISPs liable for the acts of third parties will have a disproportionate effect on small ISPs, who have to contract out more often and more extensively. This is especially true if the liability extends to the entire lifespan of the data"); *see id.* at 105 (ISPs enter into agreement with third party agents for a variety of purposes, and the proposals could deter some third parties form working with ISPs in the future); *see id.* at 91 ("[A] small ISP that lacks the resources and scale to have an internal marketing team may need to establish an ongoing relationship with a vendor to communicate with its customers about existing or new products or services").

142 *See* NTCA Comments at 65.

of devices, apps, or operating systems. Manufacturers, not ISPs, should be responsible for the security of their own devices, applications and systems."[143] Further, small carriers lack the size and scope necessary to hold much sway with third parties at the negotiating table with respect to assigning liability for data security risks. Consider small carriers' struggle to obtain access to devices operable on non-Tier 1 GSM networks, despite the overall growth in mobile wireless connections.[144] If small carriers cannot incentivize Original Equipment Manufacturers ("OEMs") like, to cite a recent example, Samsung, to release its newest devices to non-Tier 1 GSM carriers at the same time as Tier 1 GSM carriers, it is unlikely those OEMs would engage in contractual negotiations with respect to liability for data security risks.[145] Demanding extra oversight simply codifies such a competitive disadvantage to small carriers.

X. SMALL PROVIDER EXEMPTION

Those representing regional and rural carriers urge the Commission to provide relief for small providers, who will undoubtedly experience greater costs and compliance burdens. The Commission cannot ignore these burdens, nor can they credibly argue the integrity of the small provider business model would not be compromised. This is especially appropriate considering most small mobile broadband providers do not broker customer information at all.[146] CCA

---

143 CTIA Comments at 166-167

144 *See* Comments of Competitive Carriers Association, WT Docket No. 16-137 at 17-18 (filed May 31, 2016) ("CCA 19th Mobile Competition Report Comments").

145 *See id.*

146 *See* Comments of NTCA at 9; *see also* RWA Comments at 4-5 ("[A]lthough the privacy concerns are the same, the risks for small carriers are not – they make only basic use of customer data, generally do not share with or sell to third parties, and do not actively monitor data"); *see* WTA Comments at 16 (Notes that "[b]ecause of the limited size of their customer bases, these small providers largely do not use or sell customer information of any kind to third-parties").

maintains providers who do not share consumer data with third parties should be exempt from the FCC's privacy regime.[147]

In our initial comments, CCA and others provided the Commission with examples of relevant metrics to consider when defining a "small provider" according to the Small Business Administration's (SBA) definition (a provider with fewer than 1,500 employees, or 500,000 subscribers).[148] As CCA explained in its comments, an exemption for providers serving 100,000 subscribers (or connections) would not provide acceptable protection or coverage for small providers in the marketplace, and therefore would be antithetical to the Commission's values.[149] Consider the cost of data breaches alone; earlier, CCA cited to an estimate showing the notification costs associated with a data breach reach $130,000 or more for a breach touching 1,000 customers.[150] Consider the fees needed to consult with experts to define a "communications related service" as communications technology continues to evolve and touch new spheres of everyday life, or the immense data retention and organization costs implicated by Section 64.7003, and the many other associated costs small provider advocates described in painful detail throughout the record. Provider businesses serving far more than 100,000 subscribers would struggle to cope.

---

147 *See* CCA Comments at 33-34; *see also* RWA Comments at 9.

148 *See* Comments of CCA at 31; *see also id.* (considering the burdens implied by the proposed privacy rules dwarf those of enhanced transparency requirements, a 100,000 subscriber or connection threshold is inappropriate for any exemption the Commission may adopt); *see also* Small Business Broadband Deployment Act, H.R. 4596, 114th Cong (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/4596 ("H.R. 4596"); *see also* NTCA Comments at 55.

149 *See* RWA Comments at 2; see also WTA Comments at 6.

150 *Id.*

Considering escalating Congressional oversight of the Commission's privacy efforts,[151] and the demonstrated needs of small providers when crafting privacy rules, including any small provider exemption, the Commission should adopt a flexible, principles-based regime consistent with the FTC's regime. CCA agrees with the record that this would relieve the need for a small provider exemption, and streamlined oversight in this area.[152]

a. Alternatively, Small Providers Should Receive an Extension of Time to Comply With New Regulations

If the Commission declines to adopt a small provider exemption or if the adopted exemption does not provide meaningful relief or flexibility for small providers, CCA urges the Commission to allot those providers an extension of time to comply with new regulations.[153] An extension would give small providers "a window to develop compliance processes and procedures and technical solutions."[154] WISPA explains that "[s]mall providers, especially those

---

151 *See Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 114th Cong. (2016); *see also FCC Overreach: Examining the Proposed Privacy Rules: Hearing Before the Subcomm. On Communications and Technology of the House Energy and Commerce Comm.*, 114th Cong. (2016).

152 *See* RWA Comments at 6 (the proposed requirements would impose high costs on small BIAS providers, and that the burdens associated with those costs can be alleviated with targeted exemptions and compliance deadlines).

153 *See, e.g.*, RWA Comments at ii (RWA suggests a 24-month extended compliance deadline for small providers regarding notice, security, and breach notification); *see also* SBA Advocacy Letter at 4 ("Advocacy strongly supports suggestions that the FCC adopt delayed compliance schedules for small BIAS providers. Giving small providers more time to comply with the FCC's rules will allow them to spread costs and manage their limited resources in a way that will minimize harm to their ability to serve customers").

154 RWA Comments at ii; *see* WISPA Comments at 26-27 ("Companies either will need to draft training manuals or re-write them, again requiring the service of lawyers expert in privacy law. In the event reporting to the Commission is required, small broadband providers – which may not have ever been required to file annual CPNI certifications – will need sufficient time to incorporate practices that will make the certifications accurate and complete").

with a handful of employees that serve a few hundred customers, cannot be expected to simply tackle these new obligations as a part of their jobs, or find the money to pay for the expertise and documentation that would be required."[155] Indeed, an extension would take into consideration the often limited resources of smaller providers, while allowing these providers the opportunity to comply with enhanced Commission regulations.

XI. CONCLUSION

Mobile BIAS providers are expected to innovate, and to drive the U.S. economy. As the record reflects, considering the robust uptick in mobile use and the thundering demand for more advanced capabilities and service offerings, consumers expect their BIAS provider to supply (and market) faster, more innovative services in conjunction with third parties. Further, the FCC is not insulated from the business process, and should not elevate dogma over actual value to consumers at the expense of the smallest providers. The record demands that the Commission must substantially revise its proposed privacy rules. Accordingly, CCA urges the Commission to consider the aforementioned recommendations to improve consumer protection while clearly supporting mobile BIAS providers competing in the Internet marketplace.

Respectfully submitted,

/s/ Rebecca Murphy Thompson
Steven K. Berry
Rebecca Murphy Thompson
Elizabeth Barket
COMPETITIVE CARRIERS ASSOCIATION
805 15th Street NW, Suite 401
Washington, DC 20005

July 6, 2016

[155] WISPA Comments at 27.